(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－327436

(43)公開日　平成11年(1999)11月26日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０９Ｃ	1/00	６１０	Ｇ０９Ｃ	1/00	６１０Ｚ
		６２０			６２０Ｚ
Ｈ０３Ｍ	13/12		Ｈ０３Ｍ	13/12	
Ｈ０４Ｌ	1/00		Ｈ０４Ｌ	1/00	Ｂ
	9/06			9/00	６１１Ｚ

審査請求　未請求　請求項の数７　ＯＬ　（全５頁）　最終頁に続く

(21)出願番号　特願平10－133035

(22)出願日　平成10年(1998)５月15日

(71)出願人　000002945
オムロン株式会社
京都府京都市右京区花園土堂町10番地

(72)発明者　河合　武宏
京都府京都市右京区花園土堂町10番地　オムロン株式会社内

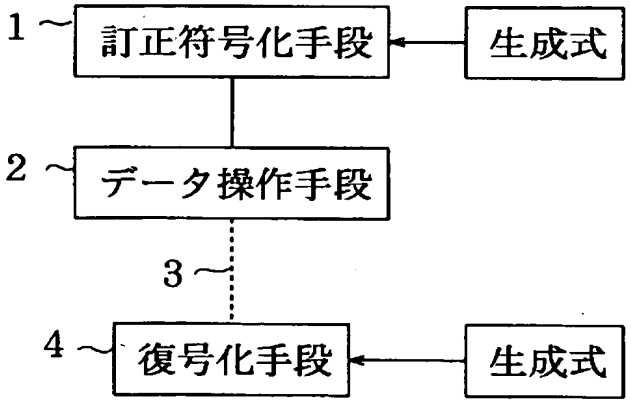
(74)代理人　弁理士　岡本　宜喜　（外１名）

(54)【発明の名称】　暗号化装置

(57)【要約】

【課題】　平文を暗号化する暗号化装置において、平文と暗号文とを１対１に対応させないようにして安全性を向上させること。

【解決手段】　入力された平文を訂正符号化手段１によって訂正符号化する。そして符号化されたデータ列を誤り訂正可能なビット数の範囲内で、データ操作手段２によって変化させる。こうすれば平文と伝送すべき暗号文とが１対Ｎに対応することとなる。この伝送されたデータ列をそのまま復号化手段４で復号化することによって、元の平文を生成することができる。



1

【特許請求の範囲】

【請求項１】　入力されたデータをブロック符号により訂正符号化する訂正符号化手段と、

前記訂正符号化手段による誤り訂正可能なビット数の範囲内で、訂正符号化されたデータをランダムに変化させることによって暗号化するデータ操作手段と、

前記データ操作手段によって操作されたデータに対して誤り訂正処理を行って復号化する復号化手段と、を有することを特徴とする暗号化装置。

【請求項２】　入力されたデータを畳み込み符号により訂正符号化する訂正符号化手段と、

前記訂正符号化手段による誤り訂正可能なビット数の範囲内で、訂正符号化されたデータをランダムに変化させることによって暗号化するデータ操作手段と、

前記データ操作手段によって操作されたデータに対して誤り訂正処理を行って復号化する復号化手段と、を有することを特徴とする暗号化装置。

【請求項３】　前記データ操作手段は、擬似ランダムデータ列を用いて操作するものであることを特徴とする請求項１又は２記載の暗号化装置。

【請求項４】　入力されたデータを暗号化して前記訂正符号化手段に出力する暗号化手段と、

前記復号化手段によって復号化された暗号化データを復号する暗号復元手段と、を更に有することを特徴とする請求項１～３のいずれか１項記載の暗号化装置。

【請求項５】　入力されたデータを訂正符号化する第１の訂正符号化手段と、

前記第１の訂正符号化手段による誤り訂正可能なビット数の範囲内で、訂正符号化されたデータをランダムに変化させることによって暗号化する第１のデータ操作手段と、

前記第１のデータ操作手段から入力されたデータを訂正符号化する第ｎ（ｎ≧２）の訂正符号化手段と、

前記第ｎ－１の訂正符号化手段による誤り訂正可能なビット数の範囲内で、訂正符号化されたデータをランダムに変化させることによって暗号化する第ｎのデータ操作手段と、

前記第ｎ～第１のデータ操作手段によって操作されたデータ列に対して夫々誤り訂正を行って復号化する第ｎ～第１の復号化手段と、を有することを特徴とする暗号化装置。

【請求項６】　前記データ操作手段の出力を伝送する有線伝送路を有することを特徴とする請求項１～５のいずれか１項記載の暗号化装置。

【請求項７】　前記データ操作手段の出力を伝送する無線伝送路を有することを特徴とする請求項１～５のいずれか１項記載の暗号化装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はデジタル通信に用いられる通信データの暗号化装置に関するものである。

2

【０００２】

【従来の技術】従来データ通信においては伝送するデータを第三者に知られないようにするために種々の暗号化装置が用いられている。従来の暗号化技術の一つとしてＤＥＳによる暗号化やＲＳＡによる暗号化が知られている。ＤＥＳによる暗号化は図５（ａ）に示すように非公開鍵を用いて伝送すべきデータ（以下、平文という）を変換して暗号文とするものであり、復号化時にはこれと同一の非公開鍵を用いて復号化するものである。又ＲＳＡによる暗号化は図５（ｂ）に示すように平文を公開鍵を用いて暗号化し、暗号文を伝送し、復号化時に非公開鍵を用いて平文に変換するものである。

【０００３】

【発明が解決しようとする課題】しかるにこのような従来の暗号化方式によれば、いずれも伝送すべき文、即ち平文とそれに対応する暗号文とが図５に示すように１対１に対応している。即ち鍵と平文及び暗号方式が同一であれば、同一の暗号文が生成されることとなる。従って平文と暗号文との対を多数入手することによって、その間の関係から鍵が見いだされてしまう可能性があるという問題点があった。

【０００４】本発明はこのような従来の問題点に着目してなされたものであって、平文と暗号文との対応を１対１とせず、１つの平文から多数の暗号文を生成できるようにして、暗号の安全性を向上させるようにすることを目的とする。

【０００５】

【課題を解決するための手段】本願の請求項１の発明は、入力されたデータをブロック符号により訂正符号化する訂正符号化手段と、前記訂正符号化手段による誤り訂正可能なビット数の範囲内で、訂正符号化されたデータをランダムに変化させることによって暗号化するデータ操作手段と、前記データ操作手段によって操作されたデータに対して誤り訂正処理を行って復号化する復号化手段と、を有することを特徴とするものである。

【０００６】本願の請求項２の発明は、入力されたデータを畳み込み符号により訂正符号化する訂正符号化手段と、前記訂正符号化手段による誤り訂正可能なビット数の範囲内で、訂正符号化されたデータをランダムに変化させることによって暗号化するデータ操作手段と、前記データ操作手段によって操作されたデータに対して誤り訂正処理を行って復号化する復号化手段と、を有することを特徴とするものである。

【０００７】本願の請求項３の発明は、請求項１又は２の暗号化装置において、前記データ操作手段は、擬似ランダムデータ列を用いて操作することを特徴とするものである。

【０００８】本願の請求項４の発明は、請求項１～３のいずれか１項の暗号化装置において、入力されたデータ

を暗号化して前記訂正符号化手段に出力する暗号化手段と、前記復号化手段によって復号化された暗号化データを復号する暗号復元手段と、を更に有することを特徴とするものである。

【０００９】本願の請求項５の発明は、入力されたデータを訂正符号化する第１の訂正符号化手段と、前記第１の訂正符号化手段による誤り訂正可能なビット数の範囲内で、訂正符号化されたデータをランダムに変化させることによって暗号化する第１のデータ操作手段と、前記第１のデータ操作手段から入力されたデータを訂正符号化する第ｎ（ｎ≧２）の訂正符号化手段と、前記第ｎ－１の訂正符号化手段による誤り訂正可能なビット数の範囲内で、訂正符号化されたデータをランダムに変化させることによって暗号化する第ｎのデータ操作手段と、前記第ｎ～第１のデータ操作手段によって操作されたデータ列に対して夫々誤り訂正を行って復号化する第ｎ～第１の復号化手段と、を有することを特徴とするものである。

【００１０】本願の請求項６の発明は、請求項１～５のいずれか１項の暗号化装置において、前記データ操作手段の出力を伝送する有線伝送路を有することを特徴とするものである。

【００１１】本願の請求項７の発明は、請求項１～５のいずれか１項の暗号化装置において、前記データ操作手段の出力を伝送する無線伝送路を有することを特徴とするものである。

【００１２】

【発明の実施の形態】次に本発明の第１の実施の形態について図１を用いて説明する。この実施の形態では、まず入力された平文を訂正符号化手段１によって符号化する。訂正符号化手段１は例えば生成式を用いてブロック符号により符号化するものであってもよく、又畳み込み符号を用いた符号化であってもよい。ブロック符号化の例として、例えばハミング符号，ＢＣＨ符号，リードソロモン符号等のランダム誤り訂正符号や、ファイア符号，短縮化巡回符号等のようなバースト誤り訂正符号がある。又畳み込み符号の例として、自己直交符号，ビタビ復号用符号，逐次復号用符号等のランダム誤り訂正符号や、ハーゲルバーカ符号，岩垂・マッシィ符号，バーレカンプ・マッシィ符号のようなバースト誤り訂正符号がある。ここでは生成式を用いた誤り訂正符号を用いて訂正符号化を行うものとする。そして符号化された文はデータ操作手段２に与えられる。データ操作手段２では訂正符号化手段１で訂正符号化が行われた際に訂正の可能な範囲内でのデータ列を変換する。即ち訂正符号化手段１による符号化であるビット数の誤りがあっても訂正可能であるとすれば、それ以下のビット数をランダムに変換して暗号化する。このデータ列操作は例えば擬似ランダム符号を用いて行うことができる。例えば誤り訂正符号によるデータ列を１００ビット、訂正可能なビット数を１０ビットとすると、１～１００までの一様な乱数を例えばＭ系列の擬似ランダム符号によって生成し、生成された擬似ランダム符号で決まるビットを逆転させる。この処理を訂正可能なビット数以下の回数（ｎ回）内で繰り返すことによってデータ列操作を行う。こうすれば入力された平文とデータ操作手段から出力される暗号文とは、１対Ｎ（$=_{100}C_n$）の対応をもつこととなる。

【００１３】このような暗号文を伝送路３を介して伝送し、受信側では復号化手段４によって復号化する。復号化手段４はデータ符号化手段１の符号化に対応した復号を行うものであり、前述した生成式を用いた場合には同一の生成式を用いて復号化する。こうすればデータ操作手段２から復号化手段４への間でデータの誤りがない場合、又は誤りがあってもデータ操作手段１で変換されたビット数＋伝送過程で生じた誤りのビット数の和が誤り訂正可能な範囲内であれば、復号化手段４で復号化することによって元のデータ（平文）に変換することができる。

【００１４】図２はこの変換の一例を示す図であり、例えば平文を「０１２３４」とし、訂正符号化手段１の処理によって例えば「０１２３４２２６６１」が生成されたものとする。データ操作手段２ではこのうちの３桁を他の数値にランダムに変換する。例えば図示のように「０９１３４５２６６１」，「５１２３９２２２６１」のように変換する。これらの暗号文を伝送路３を介して伝送し、伝送路の過程で誤りがなければそのまま復号化手段４によって符号化することにより、元の平文「０１２３４」を生成することができる。この場合には元の平文と伝送される暗号文とは１対Ｎに対向しており、１対１に対応していない。従って同一の平文に対しても使用の毎に異なった暗号文が伝送されることとなり、平文と暗号文との対を多数取得してもデータ間の関連性が低いため、元の暗号化アルゴリズムを認識することが難しく、伝送時の安全性を向上させることができる。

【００１５】次に本発明の第２の実施の形態について図３を用いて説明する。この実施の形態ではあらかじめ平文を暗号化し、これを前述した第１の実施の形態と同様に訂正符号化及びデータ操作を行うものである。即ち入力された平文は一旦暗号化手段１１によって暗号化処理が行われる。暗号化手段１１は前述した従来の暗号化処理、例えばＤＥＳやＲＳＡ等の暗号化処理を用いる。この場合には公開鍵又は非公開鍵を用いて暗号化処理を行う。そして暗号化された暗号文は訂正符号化手段１によって第１の実施の形態と同様に訂正符号化処理を行う。そしてデータ操作手段２によりデータ操作を行い、暗号文をランダムに変換する。そして伝送路３を介して復号化手段４で復号化処理を行う。こうして符号化された暗号文を暗号復元手段１２によって復元する。この場合には暗号化手段１１に対応してＤＥＳ又はＲＳＡによる復

元処理を行う。こうすれば従来の暗号化処理に加えて、訂正符号化手段による訂正符号化及びデータ列操作を行っていることにより、伝送すべき平文と伝送される暗号文との関係が更に複雑となり、これらの対を多数入手しても元の信号を復号化することは極めて困難となる。

【００１６】次に本発明の第３の実施の形態について説明する。この実施の形態では第１の実施の形態と同一の第１の訂正符号化手段１及び第１のデータ列操作手段２に更に訂正符号化を行ったものである。この実施の形態では図４に示すように第１のデータ操作手段２によってデータ列操作を加えた文を、更に生成式２を用いて第２の訂正符号化手段２１によって訂正符号化する。そして生成された訂正符号に第２のデータ操作手段２２によって同様のデータ列操作を加えて、伝送路３を介して伝送する。そして伝送した信号に対して第２の訂正符号化手段２１の訂正符号化に対応する第２の復号化処理を復号化手段２３によって行う。更に第１の訂正符号化手段１に対応した復号化処理を第１の実施の形態と同様に、復号化手段４によって復号化する。こうすれば元の平文に復号化することができる。

【００１７】尚ここでは訂正符号化処理及びデータ列操作を２回繰り返しているが、更に多数回同様の処理を繰り返してその繰り返し回数だけ復号化処理を行うようにしてもよい。又複数の訂正符号化手段の処理は同一の訂正符号化でなく、前述した種々の訂正符号化のうち異なった訂正符号化の処理を組合せて用いるようにしてもよい。こうすれば元の平文と伝送される暗号文との対応が更に複雑となり、伝送文の安全性を向上させることができる。

【００１８】尚本実施の形態ではデータ伝送路については明示していないが、有線又は無線のいずれでデータを伝送してもよいことはいうまでもない。又単にデータを大容量メモリ等に保持しておく場合にも、本発明を適用することができる。又非接触識別システムにおけるデータ伝送にこのようなデータ伝送方式を適用することができることはいうまでもない。

【００１９】

【発明の効果】以上詳細に説明したように本発明によれば、伝送すべき平文と伝送される暗号文とが１対１に対応しておらず、１対Ｎに対応しているため平文と暗号文との対を取得しても暗号化アルゴリズムを見いだすことが極めて難しくなり、データの安全性を向上させることができるという効果が得られる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態による暗号化装置の構成を示すブロック図である。

【図２】この実施の形態による暗号化装置の平文及び暗号文の一例を示す概略図である。

【図３】本発明の第２の実施の形態による暗号化装置の構成を示すブロック図である。

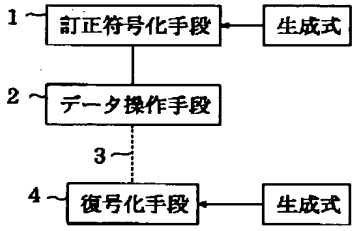
【図４】本発明の第３の実施の形態による暗号化装置の構成を示すブロック図である。

【図５】従来の暗号化装置の構成を示すブロック図である。

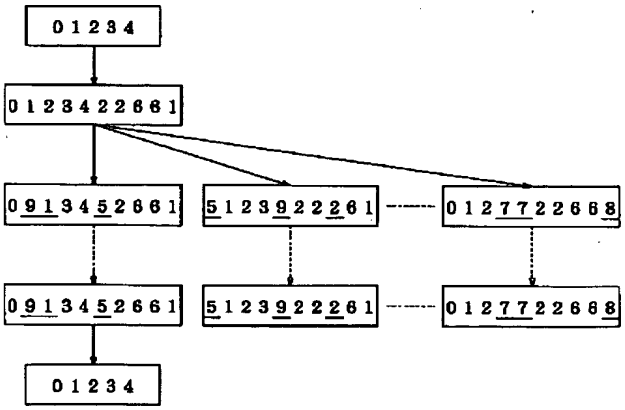
【符号の説明】

１，２１　訂正符号化手段
２　データ操作手段
３　伝送路
４，２２　復号化手段
１１　暗号化手段
１２　暗号復元手段

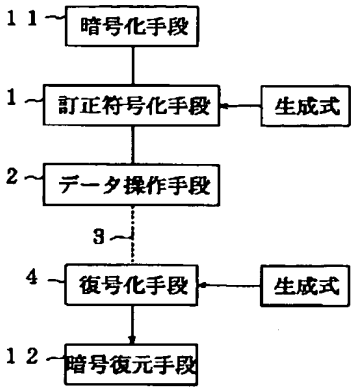
【図１】



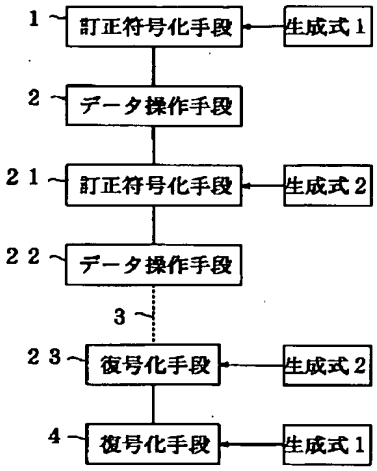
【図２】



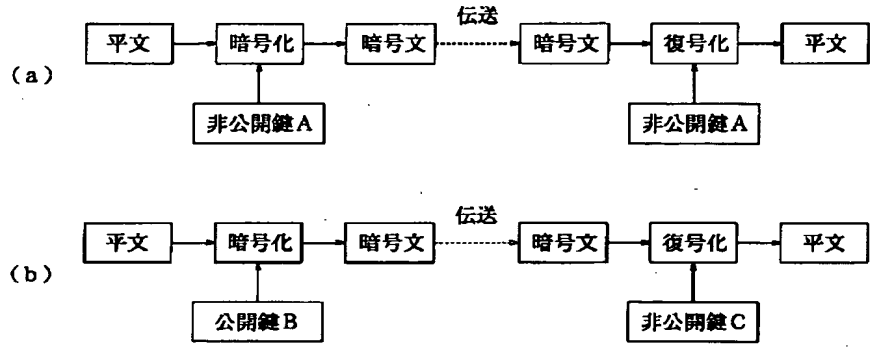
【図３】



【図４】



【図５】



フロントページの続き

(51)Int.Cl.[6]	識別記号	F I	
H04L 9/30		H04L 9/00	663Z